UNITED STATES DISTRICT COURT
FOR DISTRICT OF NEW JERSEY

EUGENE WENDELKEN, on behalf of himself individually and on behalf of all others similarly situated, Plaintiff, v. HAFETZ AND ASSOCIATES LLC, Defendant.	**CASE NO. _____** **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiff EUGENE WENDELKEN ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant HAFETZ AND ASSOCIATES LLC, ("Hafetz" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names, Social Security numbers, and insurance benefit information ("personal identifying information" or "PII").

3. On information and belief, the Data Breach occurred between July 24, 2023, and October 12, 2023, an appalling 80 days long. Following an internal investigation, Defendant

learned cybercriminals had gained unauthorized access to consumers' personally identifiable information ("PII"), including but not limited to names, social security numbers, and insurance benefit information.

4. Hafetz's breach differs from typical data breaches because it affects consumers who had no relationship with Hafetz, never sought one, and never consented to Hafetz collecting and storing their information.

5. On or about June 28, 2024– an appalling *eleven* months after the Data Breach first occurred– Hafetz finally began notifying Class Members about the Data Breach ("Breach Notice"). A sample Breach Notice is attached as Exhibit A. Plaintiff's Breach Notice is attached as Exhibit B.

6. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering it an easy target for cybercriminals.

7. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its consumers how many people were impacted, how the breach happened, or why it took the Defendant almost a year to finally begin notifying victims that cybercriminals had gained access to their highly private information.

8. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect its consumers' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed thousands of its current and former consumers.

11. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff is a Data Breach victim.

13. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and unsecure.

PARTIES

14. Plaintiff, Eugene Wendelken, is a natural person and citizen of New Jersey, where he intends to remain.

15. Defendant, Hafetz, is a New Jersey company, with its principal place of business at 609 New Road, Linwood, New Jersey 08221.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of

$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. At least one class member and Defendant are citizens of different states.

17. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

Hafetz

19. Hafetz considers itself an "independent insurance agency, specializing in employee health benefits and offering superior customer and broker services."1 Hafetz boasts that its "mission is to be the most successful provider of employee health products and services by offering our clients innovative, cutting-edge ideas tailored to meet their specific needs."[2] Hafetz boasts a total annual revenue of $5.3 million.[3]

20. Hafetz's insurance services are specialized for corporations and employers who oversee highly sensitive data. Hafetz thus must oversee, manage, and protect the PII of its clients' employees, Hafetz's consumers.

21. On information and belief, these third-party consumers, whose PII was collected by Hafetz, do not directly do any business with Hafetz.

[1] Linkedin, Hafetz and Associates, https://www.linkedin.com/company/hafetz-and-associates/ (last visited July 10, 2024).
[2] Hafetz, About us, https://hafetzandassociates.com/# (last visited July 10, 2024).
[3] Hafetz, Zoominfo, https://www.zoominfo.com/c/hafetz-and-associates/71616127 (last visited July 10, 2024).

22. As a self-proclaimed leader in its industry handling highly sensitive aspects of its clients' business, Hafetz understood the need to protect its client's employees' data and prioritize its data security.

23. Indeed, Hafetz promises in its privacy policy that it utilizes "[w]e have implemented operational, administrative, technical, and physical safeguards and procedures, including privacy and security training programs for members of our workforce, to protect your PII and ensure its confidentiality, integrity, and availability, and prevent unauthorized or inappropriate access, use, or disclosure."[4]

24. Despite recognizing its duty to do so, on information and belief, Hafetz has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Hafetz leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

The Data Breach

25. Plaintiff is unsure how Hafetz got his PII, including his name, date of birth, Social Security Number, and insurance benefit information. Regardless, in collecting and maintaining PII, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

26. On information and belief, Defendant collects and maintains consumers' PII in its computer systems.

[4] Privacy Policy, Hafetz, https://hafetzandassociates.com/insurance/privacy-policy/ (last visited July 10, 2024).

27. According to the Breach Notice, Hafetz admits that "an unauthorized person had access to the employee email accounts at various times between July 24, 2023 and October 12, 2023. Ex. A. Due to the intentionally obfuscating language in Defendant's Breach Notice, it is unclear when Defendant actually discovered this Breach, which had allowed cybercriminals unfettered access to the Class's most sensitive information for at least 80 days.

28. Following an internal investigation, Hafetz determined that the Data Breach had occurred due to numerous successful email phishing through employee email accounts. Ex. A. In other words, the Data Breach investigation revealed Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its customer's highly private information.

29. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

30. On or around June 28, 2024 –almost a year after the Breach first began occurring – Hafetz finally began notifying Class Members about the Data Breach.

31. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing consumers' PII, as evidenced by the Data Breach.

32. In response to the Data Breach, Defendant contends that it has or will be taking "implement[ing] changes to our email environment and are providing employees with additional training on how to identify and avoid suspicious emails." Ex. A. Although Defendant fails to fully expand on what these alleged "changes" are, such changes and training on suspicious emails should have been in place before the Data Breach.

33. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect customers' PII, insisting that, despite the Data Breach demonstrating otherwise, "Hafetz and Associates is committed to protecting the confidentiality and security of the information we maintain." Ex. A.

34. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity." Ex. A.

35. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

36. On information and belief, Hafetz offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

37. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

38. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they suffered and will suffer.

39. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

40. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the insurance industry preceding the date of the breach.

41. In light of recent high profile data breaches at other financial partner and provider companies, Defendant knew or should have known that its electronic records and consumers' PII would be targeted by cybercriminals.

42. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[5] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[6]

43. Indeed, cyberattacks against the financial industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the

[5] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 5, 2023).
[6] *Id.*

increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [7]

44. Cyberattacks on financial systems and banking partner and provider companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

45. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Plaintiff's Experience

46. Plaintiff received his Breach letter in early July. Plaintiff is unsure how Hafetz got his PII, including his name, date of birth, Social Security Number, and insurance benefit information.

47. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it.

48. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

49. Importantly, plaintiff does not recall ever learning that his PII was compromised in a data breach incident, other than the breach at issue in this case.

[7] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).
[8] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

50. Plaintiff suffered actual injury from the exposure of his PII —which violates his rights to privacy.

51. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the impacts of the Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

52. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Indeed, as a result of the Data Breach, Plaintiff has already spent many several months dealing with the extensive repercussions and attempting to protect himself from any additional harms.

53. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

54. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

55. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

56. Indeed, on a day following the Data Breach, Plaintiff experienced an unusual lack of phone service and observed that his phone's Wi-Fi had changed to Xfinity. When

Plaintiff attempted to log into his email to contact Xfinity, he discovered he was locked out of his account and unable access his account. As a result, Plaintiff was forced to travel to the nearest Xfinity store, where he was informed that he had suffered an identity theft and that an unauthorized individual had infiltrated his account and had successfully ported his phone number to a T-Mobile account, suggesting that his PII was now in the hands of cybercriminals as a result of the Data Breach. Further, as a result of this fraudulent porting of his phone number, Plaintiff lost the ability to utilize his phone number for at least four days.

57. Shortly after his Xfinity account experience, Plaintiff also discovered that he had suffered numerous fraudulent wire transfers totaling $27,000 from his Oceans First Bank account that he did not recognize and certainly did not authorize. As a result, Plaintiff was forced to file a police complaint regarding these wire transfers

58. Also following the Data Breach, Plaintiff discovered an unauthorized individual had accessed his American Express debit card and that another or the same unauthorized individual also attempted to access his Fidelity Investment 401k account. These unauthorized access, fraudulent wire transfers, and attempts to access Plaintiff's 401k account further suggest that his PII is now in the hands of cybercriminals as a result of the Breach.

59. Additionally and following the Data Breach, Plaintiff also discovered that he was locked out of his Amazon and Google account, with an unauthorized individual attempting to purchase gift cards through his Amazon account that he did not recognize and certainly did not authorize, further evidencing the extent of the harm this Data Breach has caused him.

60. Plaintiff has also suffered numerous fraudulent accounts being open under his name that he does not recognize nor authorize, including numerous Cashapp accounts. Upon information and belief, these fraudulent accounts are also a result of the Data Breach.

61. Finally, shortly after the Data Breach, Plaintiff has suffered a significant increase in spam texts, further suggesting that his PII is now in the hands of cybercriminals.

62. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[9] On information and belief, Plaintiff's numerous account information, including his Xfinity account, phone number, Google account, bank account, email account, and Amazon account as well as his Fidelity Investment 401k account and American Express debit account was compromised as a result of the Data Breach.

63. As a result of the Breach and the extensive fraudulent activity and identity theft it resulted in, Plaintiff has been forced to spend at least $40 to place a lock on his credit through the three credit bureaus as well as paying extra to obtain extra security on his accounts, including his AOL email.

64. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

65. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

66. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses,

[9] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

67. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

68. The value of Plaintiff's and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly

and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

69. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

70. One such example of criminals using PII for profit is the development of "Fullz" packages.

71. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

72. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

73. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices

and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

74. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

75. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

76. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

77. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

78. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

81. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

82. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data.

Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

83. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

84. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

85. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

86. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach including all those who received notice of the breach.

87. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

88. Plaintiff reserves the right to amend the class definition.

89. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of several thousand members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant were negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

90. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Classes)

91. Plaintiff realleges all previous paragraphs as if fully set forth below.

92. Plaintiff and members of the Classes entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Classes a duty to exercise reasonable care in

handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

93. Defendant owed a duty of care to Plaintiff and members of the Classes because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Classes' PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

94. Defendant owed to Plaintiff and members of the Classes a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Classes the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Classes to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

95. Defendant owed these duties to Plaintiff and members of the Classes because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's

inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Classes' personal information and PII.

96. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

97. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff's and members of the Classes' and the importance of exercising reasonable care in handling it.

98. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Classes which actually and proximately caused the Data Breach and Plaintiff's and members of the Classes' injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Classes, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Classes' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Classes have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

99. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Classes actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII

by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Classes)

100. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

101. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Classes' PII.

102. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Classes' sensitive PII.

103. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

104. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Classes.

105. Defendant had a duty to Plaintiff and the members of the Classes to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and the Classes' PII.

106. Defendant breached its respective duties to Plaintiff and members of the Classes under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Classes' PII.

107. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

108. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Classes, Plaintiff and members of the Classes would not have been injured.

109. The injury and harm suffered by Plaintiff and members of the Classes were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Classes to suffer the foreseeable harms associated with the exposure of their PII.

110. Had Plaintiff and members of the Classes known that Defendant did not adequately protect their PII, Plaintiff and members of the Classes would not have entrusted Defendant with their PII.

111. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Classes have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Contract
(On Behalf of Plaintiff and the Class)

112. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

113. Defendant entered into various contracts with its clients, including corporation and employers, to provide services to its clients.

114. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

115. Defendant knew that if it were to breach these contracts with its financial provider clients, the clients' employees, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

116. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

117. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

118. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

119. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

120. Plaintiff and members of the Class conferred a benefit upon Defendant in providing PII to Defendant.

121. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate its services to Plaintiff and the Class.

122. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

123. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective

security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

124. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class's PII because Defendant failed to adequately protect their PII.

125. Plaintiff and Class Members have no adequate remedy at law.

126. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

127. Plaintiff realleges all previous paragraphs as if fully set forth below.

128. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

129. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

130. Because of the highly sensitive nature of the PII, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

131. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII.

132. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

133. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT V
Invasion of Privacy — Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

134. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

135. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

136. Defendant owed a duty to its employees, including Plaintiff and the Class Members, to keep their PII confidential.

137. Defendant failed to protect said PII and exposed the PII of Plaintiff and the Class Members to unauthorized persons which is now publicly available, including on the dark web, and being fraudulently misused.

138. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiff and the Class Members, by way of Defendant's failure to protect the PII.

139. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class Members is highly offensive to a reasonable person.

140. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class Members PII was disclosed to Defendant as a condition of receiving services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

141. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

142. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because they had actual knowledge that its information security practices were inadequate and insufficient.

143. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when they allowed improper access to its systems containing Plaintiff's and Class Members' PII.

144. Defendant was aware of the potential of a data breach and failed to adequately safeguard their systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PII.

145. Because Defendant acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

146. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Class Members was disclosed to third parties without authorization, causing Plaintiff and the Class Members to suffer injury and damages as set forth herein, including monetary damages, fraudulent misuse of their PII and fraudulent charges; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to compensatory, consequential, and incidental damages as a result of the Data Breach.

147. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

COUNT VI
New Jersey Consumer Fraud Act
N.J.S.A. § 56:8-1, *et seq.*
(On Behalf of Plaintiff and the Class)

148. Plaintiff and members of the Classes incorporate the above allegations as if fully set forth herein.

149. The New Jersey Consumer Fraud Act (the "NJCFA"), N.J.S.A. § 56:8-1, *et seq.*, prohibits the act, use or employment by any person of any unconscionable commercial

practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression or omission, in connection with the sale or advertisement of any merchandise. The NJCFA applies whether or not any person has in fact been misled, deceived or damaged thereby. N.J.S.A. § 56:8-2.

150. Plaintiff, Defendant, and Class Members are "persons" within the meaning of N.J.S.A. § 56:8-1(d).

151. Defendant sells "merchandise," as defined by N.J.S.A. § 56:8-1, by offering IT and cybersecurity services to the public.

152. Defendant, operating in New Jersey, engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of IT and cybersecurity services in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

a. Misrepresenting material facts, pertaining to the sale of insurance services, to its clients' consumers, including the Plaintiff and Class Members, by representing that they would maintain adequate data security practices and procedures to safeguard Plaintiff's and Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts, pertaining to the sale of insurance services, to its clients' consumers, including the Plaintiff and Class Members, by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and Class Members' PII;

c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiff's and Class Members' PII with the intent that Plaintiff and Class Members rely on the omission, suppression, and concealment;

d. Engaging in unconscionable and deceptive acts and practices with respect to the sale of insurance services by failing to maintain the privacy and security of Plaintiff's and Class Members' PII in violation of duties imposed by and public policies reflected in the FTC Act;

e. Engaging in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiff and Class Members in a timely and accurate manner in violation of N.J.S.A. § 56:8-163;

f. Representing on its website that it is "commit[ed] to protecting your privacy and personal information," when, in fact, Maintech never implemented the security safeguards needed.

153. The above unlawful and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

154. Defendant knew or should have known that its data security practices were inadequate to safeguard Plaintiff's and Class Members' PII and that the risk of a data breach was highly likely. Defendant's actions in engaging in the above-listed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

155. Plaintiff and Class Members reasonably expected that Defendant would protect their PII and reasonably expected that Defendant would provide truthful statements on their website and privacy policies, and that it would be safe to provide Maintech with their information. These representations and affirmations of fact made by Defendant, and the facts they concealed or failed to disclose, are material facts that were likely to deceive reasonable consumers, and that reasonable consumers would, and did, rely upon in deciding whether or not to entrust their information to Maintech. Defendant, moreover, intended for consumers, including Plaintiff and Class Members, to rely on these material facts.

156. As a direct and proximate result of Defendant's unconscionable and deceptive acts and practices, Plaintiff and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PII.

157. Plaintiff and Class Members seek relief under N.J.S.A. § 56:8-19, including but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Date: July 15, 2024

Respectfully submitted,

By: */s/ Patrick Howard*

Patrick Howard (NJ Atty ID #02280-2001)
SALTZ MONGELUZZI & BENDESKY, P.C.
8000 Sagemore Drive, Suite 8303
Marlton, NJ 08053
Tel: (215) 575-3895
phoward@smbb.com

Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611

(872) 263-1100
(872) 263-1109 (facsimile)
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and Proposed Class